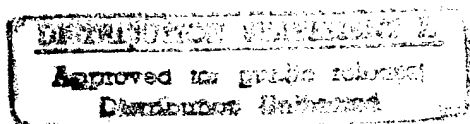NAVAL WAR COLLEGE
Newport, RI

THE IMPACT OF THE "MILLENNIUM BUG" ON COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS AND INTELLIGENCE (C^{4}I) INFRASTRUCTURE

by
Glenna L. Spencer
LCDR   USNR

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Operations Department.
The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

DTIC QUALITY INSPECTED 4   Signature: _Glenna L. Spencer_

13 June 1997

Paper directed by Captain George Jackson
Chairman, Department of Joint Military Operations

Alexander R Saunders II   3/6/97
Faculty Advisor   Date
Capt Alexander Saunders II

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:
JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI   02841-1207

8. Title (Include Security Classification): The Impact of the "Millennium Bug" on Command, Control, Communications, Computers and Intelligence (C4I) Infrastructure. (U)

9. Personal Authors: Lieutenant Commander Glenna L. Spencer, US Naval Reserve

10. Type of Report: FINAL

11. Date of Report: 7 Feb-1997

12. Page Count: 23

13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper: Command, Control, Communications, Computers, Intelligence, Millennium Bug, Year 2000 Problem

15. Abstract: The year 2000 problem will impact on virtually all aspects of our high tech world. The problem is simple, but the consequences are catastrophic and far reaching. The year 2000 is easily the worst information management crisis of all time. The impact of the "Millennium Bug" on Command, Control, Communications, Computers and Intelligence (C4I) infrastructure will be the lack of the availability of some systems and the lack of confidence in the information produced by the systems that are left.

16. Distribution / Availability of Abstract:	Unclassified	Same As Rpt	DTIC Users
	X		

17. Abstract Security Classification: UNCLASSIFIED

18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. Telephone: 841-6461

20. Office Symbol: C

ABSTRACT

The year 2000 problem will impact on virtually all aspects of our high tech world. The problem is simple, but the consequences are catastrophic and far reaching. The year 2000 is easily the worst information management crisis of all time. The impact of the "Millennium Bug" on Command, Control, Communications, Computers and Intelligence (C4I) infrastructure will be the lack of the availability of some systems and the lack of confidence in the information produced by the systems that are left.

TABLE OF CONTENTS

INTRODUCTION

Some people expect the year 2000 problem to be the most catastrophic information management crisis of all time. I do not prescribe to this "Chicken little -- the sky is falling" school of thought. The Year 2000 problem is what happens to computer systems with two digit year codes when the year 2000 starts. The computer performs basically simple mathematical calculations to determine time passage. The computer with a two digit year such as "00" will assume that "00" is less than "96" (a basic mathematical assumption), assigning "00" as 1900 instead of 2000. The Year 2000 problem will impact on all areas of our high tech world. The impact of the "Millennium Bug" on Command, Control, Communications, Computers and Intelligence (C4I) infrastructure will be the lack of the availability of some systems and the lack of confidence in the information produced by the systems that remain. It will be expensive and labor intensive to fix the year 2000 problem. Military managers need to start working immediately on this problem. Y2K is not an arbitrary deadline that can slip. Many computer programs throughout the world will turn into "pumpkins" at the stroke of midnight on 31 December 1999 if the problem goes without correction. It will be a monumental task. There is just under three years left which is not much time to fix a problem of this magnitude. Due to the limited amount of time available not all systems will be fixed. The complexity of the problem requires prioritization of systems as to the criticality. In order for Operational Commanders to accomplish their missions, systems will need to be fixed, replaced or eliminated. Due to the drain on the limited work force and monetary resources, Research and Development (R&D) projects will suffer from cancellations or delays. All systems will require evaluation and prioritization to determine the extent of the problem to

include the hardware fixes. This is truly a world-wide problem with a finite amount of resources available. As the deadline approaches conflict will arise from a lack of resources available. The U.S. government and military Services are only a small subset of the systems affected by the "Millennium Bug." All systems that interact with each other require correction at the same time. Systems not corrected that attempt to interact with corrected systems will fail or faulty information will pass between them. A critical step in the solution of the Y2K problem is to test and evaluate the system, verifying the correction of all two digit year codes. In most cases the systems will be operating concurrently while making the year 2000 changes. The process is overwhelming when you consider the myriad of systems operating within all the industrial countries in the world and specifically within all branches of the U.S. government. The U.S. military Services are a very small subset of the overall year 2000 problem. We are dependent on computers for everything from administration, pay, weapon systems, as well as satellite guidance. The age and complexity of many of the systems that we depend upon daily complicates the problem. In addition we continue to rely heavily on many of the legacy systems from the 1960's and 1970's. Over the years many different computer programmers have incorporated patches to the legacy systems. Therefore there is little or no documentation on the computer coding.

There are no federal funds designated for the Y2K problem. Funding will have to be redirected from other sources.[1] Last year Congress kicked into high gear with several subcommittee meetings held to determine the extent of the problem and educate the public.

---

[1] U.S. Congress, House, Science Committee, Technology Subcommittee and U.S. Congress, House, Government Reform and Oversight Committee, Government Management, Information and Technology Subcommittee, Solving the Year 2000 Computer Problem, Hearings (Federal Information Systems Corporation, Federal News Service, 1996)

As a result, Congress required Y2K budgetary requests be included in the 1998 budget. Unfortunately the Y2K problem cannot wait until 1998 to start finding, fixing and testing computer systems. Since each system is different, some will require more effort than others depending on the age and complexity. C4I systems are extremely vulnerable to the Y2K problem. There are many "stove pipe" C4I systems used within all the various Services. The "C4I for the Warrior" concept inputs data from the various "stove pipe" systems into a "translator" to combine the information into a universal battle space picture. When multiple systems are contributing to a single system, the possibility of erroneous data increases substantially. The faulty information would become incorporated into the system and it would be virtually impossible to determine the source or the existence of corrupted information. Since the systems have been operational for an extended period of time, the Commander assumes the information received from C4I systems is accurate. Upon entering the new millennium the information received from the C4I systems loses credibility. With the loss of confidence in the information the commander will lose some of the timeliness and usability of the information. There will be a period of time when information will require verification. Many of the systems that the commander has come to rely upon will require elimination due to the age and complexity of the system. In addition, the commander will have a learning curve once the replacement systems are brought on line. Due to the new systems the commander must learn and the lack of confidence in the information produced by the older systems, the speed of the decision making process will suffer. This could be deadly in our high tech world where milliseconds can mean the difference between life and death.

THE YEAR 2000 PROBLEM

The "Millennium Bug" which is also known as the Year 2000 crisis, Year 2000 (Y2K)

problem. In essence, the Y2K problem is what happens to computer systems with two digit

year codes when the year 2000 starts. There have been predictions of mild inconveniences

to catastrophic meltdowns. What is all the commotion? The computer performs basically

simple mathematical calculations to determine time passage. The computer with a two digit

year such as "00" will assume that "00" is less than "96" (a basic mathematical assumption),

assigning "00" as 1900 instead of 2000. When a computer system incorrectly interprets "00"

as 1900, computers will fail in one of three ways: they will reject legitimate entries, simply

will not run or they will compute erroneous results.[2] Correcting a date code is relatively easy

for a programmer. What makes the problem so monumental is that date coding is embedded

in virtually every computer program hundred of times. If a two digit year code goes without

correction, the whole system can come to a screeching halt or faulty information is

generated. Date coding is an essential part of almost every program, such as programs used

for mortgage payments, retirement eligibility, pay, and "smart weapons." To understand how

the problem developed you have to go back to the 1960's when computer programmers

thought that 12K of memory would last a lifetime.[3] To save memory space they adopted a

six digit date code (yy,mm,dd). The six digit code may not seem like much of a savings from

an eight digit date code (yyyy,mm,dd), but when there are hundreds to thousands of date

---

[2] Sally Kratzen, "Statement," U.S. Congress, House, Science Committee, Technology Subcommittee and U.S. Congress, House, Government Reform and Oversight Committee, Government Management, Information and Technology Subcommittee, Solving the Year 2000 Computer Problem, Hearings (Federal Information Systems Corporation, Federal News Service, 1996)
[3] Lisa Corbin, "The Year 2000 Problem," Government Executive, May 1996, 19-20, 25-27.

codes imbedded in a large program, the savings are significant. Memory space is no longer a problem, but the date code format did not change from the six digit format. The original programmers did not expect that the systems would be operating into the year 2000. The newer computer systems have standardized to a four digit year code to accommodate the turn of the century.

When the manufacturer wants to update or correct a program on a PC, they typically replace the old program with a new updated program. The manufacturer periodically releases new versions eliminating the need to patch the program. Therefore, PC's are not a significant area of concern in the Y2K problem. The problem becomes huge when you consider that many of our mainframe legacy computer systems from the 1960's and 1970's are still in existence. Legacy main frame computers differ from PC's in that the operating systems receive patches to update or correct problems, rather than releasing new versions. Over the years many different programmers incorporated patches with little or no documentation on the computer coding. To further complicate the problem, the majority of the original programmers have retired or moved to other companies. The maintenance and operation of many of our defense systems is conducted by individuals who were not alive when the original system was first developed. Taskforce 2000[4] member Nick Land listed some of the problems the year 2000 has already caused:

> *Three major airlines have already decided to stand down all flights for 24 hours on New Year's Eve 1999, because even if their own computers are sorted out in time, they cannot be sure that other aircraft and air traffic control systems will work correctly. The global Positioning Satellite, which directs ships, planes, tanks, and cruise missiles to their targets, will reset its date to January 06, 1980, because of a*

---

[4] "The only governement (U.K.) sponsored organization of its type in the world currently devoted to publicising the Year 2000 problem." Andy Woodcock, "Millennium Computer melt-down 'threatens Euro'," The Press Association Limited, 12 September 1996.

2000-related fault. Credit cards with expiration dates in 2000 have been withdrawn because the point of sales machines do not recognize them. A major food retailer's computers automatically rejected tins of corned beef with sell dates in 2000, believing they were a century old. Disastrous potential consequences of failing to take action include: Bills being sent out for interest payments on 99 years worth of overdraft. Great-grand parents aged 104 being told to report for school by computers that think they are four-year old toddlers. [5]

The Y2K problem is not limited to computers.

"It exists in chips, in hard-wired systems that control all sorts of things, from traffic lights and security systems down to the video-recorder in your house. At the other extreme, there are chips controlling, for example, nuclear power stations."[6]

Congress has received estimates to fix this problem as high as $30 billion for the federal government alone, $600 billion worldwide, and $300 billion in the U.S. primarily in the private sector.[7] It is clear that the extent of this problem and the overwhelming amount of coding involved could easily result in missing a two digit year code. Since it is easy to miss a two digit year code and when making changes to coding oth roblems often surface, an extensive test and evaluation period is critical to the process. The addition of an extensive testing and evaluation process, will shorten the available time to correct the Y2K problem even more. In most cases the system will be operating concurrently while making the year 2000 changes. Sally Kratzen Office of Management and Budget (OMB) gives us an apt

---

[5] Andy Woodcock, "Millennium Computer melt-down 'threatens Euro'," The Press Association Limited, 12 September 1996.
[6] Ibid.
[7] U.S. Congress, House, Science Committee, Technology Subcommittee and U.S. Congress, House, Government Reform and Oversight Committee, Government Management, Information and Technology Subcommittee, Solving the Year 2000 Computer Problem, Hearings (Federal Information Systems Corporation, Federal News Service, 1996)

description, "Some have invoked the analogy of rebuilding a rocket ship while it is on its way to the moon."[8]

This could be our first legal computer virus.[9] Consider a definition of a computer virus to be computer coding that causes the computer system to stop functioning or to generate inaccurate data. Y2K problem can produce incorrect computations that can corrupt data and crash systems like a computer virus. Unfortunately an anti-virus program would not be useful since the Y2K "virus" does not alter operating systems or destroy data. Simply put, there is not enough information in a two digit year code for the computer to correctly interpret and process the information.

Military Impact:

The military is dependent upon computers for all aspects of our daily life. We have many 1960's and 1970's legacy systems written in antiquated languages for everything from administration, logistics and weapons systems.

> "Experts warn that the date-code problem also will affect software embedded in DOD's one-of-a-kind weapons systems. 'Where DOD is unique is in the embedded software in our weapons systems--in missiles, tanks, planes and ships,' Anthony Valletta, deputy to the assistant secretary of Defense for C3I, said at a recent conference. 'Obviously, we can't take the chance of our warfighting systems failing because they process a date incorrectly, so they all must be checked.'"[10]

---

[8] Sally Kratzen, "Statement," U.S. Congress, House, Science Committee, Technology Subcommittee and U.S. Congress, House, Government Reform and Oversight Committee, Government Management, Information and Technology Subcommittee, Solving the Year 2000 Computer Problem, Hearings (Federal Information Systems Corporation, Federal News Service, 1996)

[9] Darryl K. Taft, "Toward the year 2000 -- Battling a global computer virus," Computer ResellerNews, 06 May 1996.

[10] Paul Constance, "DOD chiefs fear fixing data code in weapons systems will be tough," Government Computer News, 13 May 1996, 3.

Mitre Corporation analyzed nine DOD command and control systems, and two logistics

systems and found that there is a total of 5.4 million lines of code among these few systems.

DOD's system inventory could amount to several hundred million lines of code.[11] Within

the millions of lines of codes are thousands of date references. Several of the computer

companies have developed search engines for COBOL and a few other widely used computer

language programs to find the date references. IBM has made available it's COBOL family

of compilers, conversion aids, structuring facilities, workstation tools, and other test tools.

The problem is that the search engines only find the faulty date codes, programmers familiar

with the computer language still have to run the software. The programmers have to

manually make the changes in the individual lines of code. There are no search engines

available for many weapons systems or other legacy systems written in obscure and archaic

computer languages. Each line of computer code requires a manual search by a legion of

programmers to find all of the embedded date coding. The problem is not limited to the

computer systems. The Y2K problem exists in chips, in "firm-ware" that control a myriad of

things like missiles and other weapons. It could be impossible to replace chips that are no

longer in production. The most critical systems will receive the available resources. The

elimination of some of the legacy systems is due to the limited resources available and the

magnitude of the problem. The U.S. government and military are not the only users of the

limited resources, but quite literally the entire world will need to fix the year 2000 by the

same dead line. To further complicate the problem, DOD does not have 1997 funds

designated to fix the Y2K problem. Until the funds are made available in 1998 the funding

---

[11] Ibid.

will have to come from other sources. The conversion will likely come about at the expense

of the system development projects.[12]

This is not a new problem and the resources available are: 1) <u>Civilian companies</u> who

are available to consult, assess and recommend solutions. Many computer companies have

found it lucrative to enter into the solution of the year 2000 problem. The average cost is $1

per line of code. The Mitre corporation's report to DOD stated that it could cost up to $8.52

per line of code for weapons systems.[13] The closer you get to the deadline the more

expensive it will become, due to supply and demand. DOD will have to remanufacture chips

used in hard-wired systems or scrap some of its legacy systems.   The civilian companies are

an important resource, but with the magnitude of the problem it is not only a factor of time

but of staggering cost. 2) <u>Federal and state agencies</u> are offering help to share their

information. The Assistant Secretary of Defense for Command, Control, Communications

and Intelligence (C3I) is currently in the process of drafting a management plan for the

military.[14] Each of the Services now has a designated year 2000 coordinator who has briefed

senior officials at the Pentagon.[15] The Social Security Administration (SSA) started

working the problem in 1989.[16] SSA began repairing databases and searching 30 million

lines of code, estimated to take 300 work years.[17] SSA expects to complete the corrections

---

[12] William Jackson, "There's no extra money for 2000 code fixes, officials say," <u>Government Computer News</u>, 19 February 1996, 16.

[13] John Moore and Allan Holmes, "Year 2000 causes double trouble for feds," <u>Federal Computer Week</u>, 01 April 1996, 1, 109.

[14] "DOD Drafting Management plan for year 2000 computer efforts," <u>Phillips Business Information</u>, 18 July 1996.

[15] Paul Constance, "DOD chiefs fear fixing data code in weapons systems will be tough," <u>Government Computer News</u>, 13 May 1996, 3.

[16] Allan Holmes, "SSA's Adams focuses on Year 2000," <u>Federal Computer Week</u>, 10 June 1996, 24, 27.

[17] William Jackson, "There's no extra money for 2000 code fixes, officials say," <u>Government Computer News</u>, 19 February 1996, 16.

and start testing in late 1998. When the year 2000 starts, it will have taken SSA ten years to find, fix and test the Y2K problem! SSA is only one agency among many world-wide.

> "Preliminary assessments by DOD and industry experts indicate that hundreds of systems for planning, supplying, mobilizing and executing a mission could fail if their date fields aren't fixed and tested well in advance. In a network environment, date-change errors would have a domino effect that would cripple the nation's first response to aggression, Pentagon officials said."

World Impact:

If the U.S. has a slow start, then most assuredly the rest world will be behind us in correcting this problem. The world seems to be waiting to see how we handle the problem. Canada's marketplace, estimated at $2-$3 million US dollars for Y2K problem repair.[18]

> Britain is £15 billion and £400 billion estimated world wide will be required to correct the year 2000 problem. Taskforce 2000 (an international committee) expects that by not taking action in time, 10% of all businesses will fail. Taskforce 2000 estimates that 90% of major British organizations have done nothing to combat the problem compared to 65% in the US, 96% in Europe and 99% in the Far East. "Millions of computer records could be scrubbed clean, credit cards rendered invalid and timer programs for traffic lights, power stations, industrial fridges and public transport systems sent haywire."[19]

This is truly a universal problem affecting all industrialized countries throughout the world. Brett Proud, Manager of Keane Canada Inc.'s, (a Y2K consulting firm), said "the enormity of the problem is illustrated by the work Keane is doing for a large Canadian bank. The job will take 90 work-years to complete and cost $30-$40 million."[20] Corrected systems require protection from systems that have not completed the correction process. The world financial

---

[18] Mark Evans, "Canada: The profit clock is ticking on 2000 countdown," Financial Post, 08 May 1996, 22.
[19] Andy Woodcock, "Millennium Computer melt-down 'threatens Euro'," The Press Association Limited, 12 September 1996.
[20] Mark Evans, "Canada: The profit clock is ticking on 2000 countdown," Financial Post, 08 May 1996, 22.

network is highly vulnerable since world banks conduct thousands of transactions a day with banks all over the world. All systems within a network require correction or corrupted information can pass into "corrected" systems. Corrupted information passed between systems would send financial institutions into chaos. A two digit year code could cause enormous amounts of interest paid and cause systems to crash. Insurance companies may face terrible miscalculations with life insurance policies.[21] The Y2K problem will affect the stock market. The companies that have prepared for the year 2000 and the companies that are part of the lucrative Y2K market will see their stock increase. Companies that fail to correct the problem could be put out of business or lose value. Y2K will likely cause a change in the world market.

---

[21] Ibid.

Command, Control, Communications, Computers and Intelligence For The Warrior (C4IFTW)

"The capability of the Warrior to respond and coordinate horizontally and vertically to prosecute effectively and successfully any mission in the Battlespace is the essence of the C4I for the Warrior concept."[22]

Interoperability:

A goal of 100% interoperability is an essential element to the CJCS C4IFTW[23] to enhance operational flexibility. The Blackhawk shoot down over Iraq illustrates what can happen if interoperability fails to occur. The Blackhawk disaster could have been prevented if all of the data available had been incorporated into an all inclusive battlespace[24] picture.

> *"... some evidence suggests that the AWACS crew lost track of the two helicopters in a hand-off among crew members. According to the report, 'The Blackhawks initially were in contact with the Air Force AWACS plane monitoring the area, but were flying so low that the AWACS radar lost contact with them. When they reappeared on the radar, another air controller aboard the AWACS did not recognize them and summoned the F-15s to investigate. The fighters identified them as Iraqi Hinds. The controller asked them to make additional passes to confirm the identification, which they did. After several more passes, the F-15s were told to fire on the helicopters.'"*[25]

Blue on Blue incidents are minimized if the commander has an accurate battlespace or infosphere.[26] Interoperability enables joint operations between all Services. The

---

[22] Office of Joint Chief of Staff, <u>C4I for the Warrior</u>, (Washington, DC: GPO, 12 June 93), 2.

[23] Ibid.

[24] *"The Warriors battlespace is any area over which the warrior exercises control or has a military interest. ... an integrated picture of ground, air, maritime, space and special operations being conducted in the battlespace."* Office of Joint Chief of Staff, <u>C4I for the Warrior</u>, (Washington, DC: GPO, 12 June 93), 9.

[25] James Armstrong, "Designing, Testing, and Using C4I Systems: What causes the disconnects and what can be done about them?" Unpublished Research paper, U.S. Naval War College, Newport, RI: 1994, 60. Quoted from Thomas E. Ricke, "US Fighters Accidentally shoot Down Two American Helicopters over Iraq," Wall Street Journal, 15 April 1994, 10.

[26] *"Infosphere is a global network of military and commercial communications systems and networks linking informational data bases and fusion centers that are accessible to the warrior anywhere, anytime, in the*

individual Service's C4I system inputs information to a Joint Universal Data

Interpreter (JUDI) which fuses the input into one all inclusive battlespace picture.

> *"Fusion is the process of receiving and integrating all-source, multimedia, and multiformat information to produce and make available to the Warrior and accurate, complete, and timely summary of essential information required for successful prosecution of operational objectives. Fused information is more valuable to the Warrior than information received directly from separate, multiple sources to degree that it provides the Warrior with 'real truth.' The C4I for the Warrior concept remains committed to the Warrior's need for a fused real time, true representation of the Warrior's battlespace-- an ability to order, respond and coordinate horizontally and vertically to the degree necessary to prosecute his or her mission in that battlespace."[27]*

This assumes that the information coming in is accurate. The adage of garbage in -- garbage

out, can have deadly results for the military commander. Interoperability of individual

systems to create an infosphere is a synergistic process. When numerous systems are

inputting information during joint or combined operations it compounds the possibility of

erroneous information becoming incorporated into the infosphere. In combined operations

our allies' C4I systems require Y2K problem correction and testing, just as our systems do to

ensure accurate information. Even if they fix the Y2K problems the system loses credibility

to the commander. The information will be verified until the level of confidence returns.

When the commander doubts the information or must verify the information received from

the C4I system the time required for the decision making process increases. In joint

operations each Service has their own "stove pipe" system. Each "stove pipe" system must

correct the Y2K problem separately and accurately. The possibility of erroneous information

---

performance of any mission. The infosphere provides the world wide communications backbone and information support to the joint forces and warriors at any level." Office of Joint Chief of Staff. C4I for the Warrior, (Washington, DC: GPO, 12 June 93), 10.

[27] Office of Joint Chief of Staff, C4I for the Warrior, (Washington, DC: GPO, 12 June 93), 13, 4.

increases when multiple systems are inputting information through a translator to create an infosphere and an all inclusive battlespace picture. The biggest impact on the C4IFTW will be to delay the system from being completed on schedule. Due to the demands placed on the programming resources the C4IFTW will in all likelihood be pushed aside until the corrections for the year 2000 problems are completed.

Information Quality:

Erroneous information incorporated in the battlespace picture becomes a synergistic process also, further corrupting the picture. The Y2K problem could affect the quality of the information by degrading several of the information quality criteria.[28] 1) Geosynchronous systems that input the wrong location or time will significantly degrade the accuracy of the information. The theater of operations time and space calculations will be faulty. The Global Positioning System (GPS) was used extensively in the Gulf war.

> "*Using GPS, virtually every friendly unit knew and reported their location with pinpoint accuracy. . . . The more than 5000 GPS receivers deployed to the Gulf, were used throughout the theater to assist forces at sea, on land, and in the air. For example, GPS fixed navigational positions during mine clearing operations and provided launch coordinates for ships firing TLAM [Tomahawk Land Attack Missile]. Among other uses, GPS guided maneuver units, helped minimize fratricide, registered artillery ad precisely located land mines.*"[29] The GPS is a time-based network of 24 satellites in synchronized orbit. Each satellite constantly transmits time-tagged data bits over broadband radio frequencies to tell where it is a precisely what time. The GPS will suffer from a year 2000-related problem. The satellite timing mechanism measures time in one-week blocks of seconds. Week 1 was Jan. 6, 1980. Unfortunately their clocks hold only 1,024 weeks. On Aug 22 1999 the satellites will transmit time data as week 1--Jan. 1980. "This is could throw some receivers 'way, way off' and give bizarre location readings.*"[30]

---

[28] Office of Joint Chief of Staff, JCS Pub 6-0, <u>Doctrine for C4 Systems Support to Joint Operations,</u> (Washington, DC: GPO, 30 May 95), 1-5.

[29] James Armstrong, "Designing, Testing, and Using C4I Systems: What causes the disconnects and what can be done about them?" Unpublished Research paper, U.S. Naval War College, Newport, RI: 1994, 62-63. Quoted from U.S. Department of Defense, "Conduct of the Persian Gulf War: Final Report to Congress, (Washington, DC: GPO, April 1992), T-227.

[30] Deck, Stewart, "Year 2000 syndrome strikes again," <u>Computerworld,</u> 22 July 1996, 8.

This illustrates the vulnerability of system controlled by geosynchronous navigation to the Y2K problem. The satellites change orbit slightly each day and the receivers are programmed to find and interpret the signal based on the date. If a geosynchronous system fails to calculate the correct date it can give incorrect locations or fail completely. 2) Timeliness of the information is compromised if the commander receives erroneous data or questions the data. If the commander loses confidence in the accuracy of the information, the information for all practical purposes is false. In either case the commander is forced to verify or discount the information that would affect the timeliness. 3) Usability & 4) Completeness is reduced due to conflicting information or discounted information, creating gaps or incomplete data. At a minimum, the erroneous information is buried and it would be even more difficult to identify false information. A system crashing is preferable to erroneous information since the operator is instantly aware of a problem when the system crashes. Faulty information inputted into a system it is not as readily apparent. The commander uses the information from the C4I systems to develop a plan. Faulty information creates faulty plans. Even a slight error could cause tragic results,

> "During the Persian Gulf War, a software error in the command and control complex of the Patriot missile system was responsible for throwing off the radar's timing by one-third of a second, causing the patriot to miss an incoming Iraqi Scud missile that killed 28 soldiers and wounded 97 in Saudi Arabian barracks."[31]

---

[31] James Armstrong, "Designing, Testing, and Using C4I Systems: What causes the disconnects and what can be done about them?" Unpublished Research paper, U.S. Naval War College, Newport, RI: 1994, 58. Quoted from Carol Minton. "War Stories on the Software Testing Front," MIDRANGE Systems, 11 February 1994, 28.

CONCLUSION

The task of the military leaders to ensure that we pass uneventfully into the next millennium is unarguably daunting. The time to act is now. Mr. Miller, President of the Information Technology Association of America said that, "The Year 2000 software conversion is arguably the largest and most complex global information management challenge society has ever faced. The schedule will not slip on this one. Line by line, program by program, we have to face this date change situation head-on."[32] Every computer system must be assessed to determine the impact of the Y2K problem. DOD systems are only a very small subset of all of the systems impacted by the year 2000 problem. The U.S. government will prioritize the allocation of resources. DOD systems could be farther down on the priority list than the world financial network or the stock market if determined to be more critical to our country's survival. The limited resources will be drawn upon by "all the countries in the industrialized world." Due to the resource and time constraints, some of the older systems cannot be fixed in time. Critical systems will be fixed or replaced, some of the legacy system will be eliminated. Isolation of the newer systems not affected by the year 2000 problem and the corrected systems will minimize the possibility "cleaned" systems receiving corrupted information. A critical step in the process is an extensive test and evaluation period to verify that all year 2000 related problems are corrected. Commanders need to be educated on the problems created by passing into the new millennium. The impact of the "Millennium Bug" on C4I infrastructure will be the lack of the availability of some systems

---

[32] Harris N. Miller, "Statement," U.S. Congress, House, Science Committee, Technology Subcommittee and U.S. Congress, House, Government Reform and Oversight Committee, Government Management, Information and Technology Subcommittee, <u>Solving the Year 2000 Computer Problem</u>, Hearings (Federal Information Systems Corporation, Federal News Service, 1996)

and the lack of confidence in the information produced by the remaining systems. Mistakes in our C4I information systems can have deadly results. The information from the C4I systems requires a verification period. The verification period starts in the test and evaluation phase and continues into the new millennium, ensuring the C4I for the warrior infosphere is reliable. Proactively assessing, fixing or replacing systems will minimize the length of the verification period and provide the confidence needed to the commander utilizing C4I systems. Now is time to squash the "Millennium Bug!"

BIBLIOGRAPHY

Anthes, Gary H. "Feds face year 2000 crisis." Computerworld, 22 April 1996, 1.

_____. "Feds garner failing grades for year 2000." Computerworld, 05 August 1996, 15.

Armstrong, James E. "Designing, Testing, and Using Command, Control, Communication, Computers and Intelligence (C4I) Systems: What causes the disconnects and what can be done about them?" Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1994.

Barmann, Timothy C. "Computer firms cash in on two-digit time bomb." The Providence Journal, 22 September 1996, pp. F:1-2.

_____. "How Rhode Island is dealing with the year-2000 glitch." The Providence Journal, 22 September 1996, p. F:2.

Bender, Bryan. "Senate Bill sets aside $5 million to study 'Year 2000' solutions." Phillips Business Information, 25 June 1996.

Bowdish, Randall G. "The Revolution in Military Affairs: The Sixth Generation." Military Review, no. 6, November-December 1995, pp. 26-33.

Constance, Paul. "DOD chiefs fear fixing data code in weapons systems will be tough." Government Computer News, 13 May 1996, 3.

_____. "Year 2000 date-code glitch in the bag." Government Computer News, 24 June 1996, 61.

Corbin, Lisa. "The Year 2000 Problem." Government Executive, May 1996, 19-20, 25-27.

Davis, Lanny J. "A look At. . . The Computer Calendar Crisis: Countdown to a Meltdown; Before the Year 2000, We have to spend billions to fix a very strange glitch." The Washington Post, 15 September 1996, p. C:03

Deck, Stewart. "Year 2000 syndrome strikes again." Computerworld, 22 July 1996, 8.

"DOD Drafting Management plan for year 2000 computer efforts." Phillips Business Information, 18 July 1996.

Dorobek, Christopher J. "4 agencies earn A's on 2000 report card; House panel gives 14 agencies D's and F's." Government Computer News, 05 August 1996, 1.

_____. "Congress demands specific action on date-code repair." Government Computer News, 23 September 1996, 8.

_____. "Congress takes agencies in hand to solve date dilemma." Government Computer News, 15 July 1996, 80.

_____. "White House gets Hill to relent on demand for year 2000 plans." Government Computer News, 07 October 1996, 57.

Evans, Mark. "Canada: The profit clock is ticking on 2000 countdown." Financial Post, 08 May 1996, 22.

Hemmerick, Steve. "Software glitch could be million-dollar pain; Year 2000 problem creates expensive race against time." Pensions & Investments, 05 August 1996, 3.

Hoffman, Thomas. "Timing is right for Cobol Programmers." Computerworld, 11 March 1996, 10.

Holmes, Allan. "Bill seeks year 2000 compliance." Federal Computer Week, 20 May 1996, 14, 20.

_____. "DOD nixes noncompliant-gear buys." Federal Computer Week, 20 May 1996, 8.

_____. "SSA's Adams focuses on Year 2000." Federal Computer Week, 10 June 1996, 24, 27.

Houser, Walter R. "Will New Year's Day 2000 come as a welcome relief?" Government Computer News, 07 October 1996, 23.

Jackson, William. "There's no extra money for 2000 code fixes, officials say." Government Computer News, 19 February 1996, 16.

Journal-Bulletin Wire Reports, Washington. "Apocalypse soon: Federal agencies race to ready computers for the year 2000." The Providence Journal, 22 September 1996, pp. F:1-2.

Keuffel, Warren. " Coping with the year 2000 rollover." Software Development, August 1996, 23-24.

Kratzen, Sally. "Statement," U.S. Congress. House. Science Committee. Technology Subcommittee and U.S. Congress. House. Government Reform and Oversight Committee. Government Management, Information and Technology Subcommittee. Solving the Year 2000 Computer Problem. Hearings. Federal Information Systems Corporation, Federal News Service, 1996.

Lapolla, Stephanie. "IBM leads way in preparations for year 2000." PCWeek, 20 November 1995, 39-40.

Lowenstein, Roger. "The Year 2000 and the CEO's Big Secret." Wall Street Journal, 25 July 1996, p. C:1.

Miller, Brian. "Millennium Arrives Early." Government Technology, September 1996, 1, 46.

Miller, Harris N. "Statement," U.S. Congress. House. Science Committee. Technology Subcommittee and U.S. Congress. House. Government Reform and Oversight Committee. Government Management, Information and Technology Subcommittee. Solving the Year 2000 Computer Problem. Hearings. Federal Information Systems Corporation, Federal News Service, 1996.

Moore, John and Allan Holmes. "Year 2000 causes double trouble for feds." Federal Computer Week, 01 April 1996, 1, 109.

Mosig, Joanne M. "Command, Control, Communication, Computers and Intelligence (C4I) in Revolution." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1996.

Office of the Joint Chiefs of Staff. Joint Command, Control, Communications, and Computers Systems Descriptions, Volume II. Washington: 1995.

_____. JCS Pub 6-0, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations. Washington, DC: GPO, 30 May 95.

_____. C4I for the Warrior. Washington, DC: GPO, 12 June 93.

Olsen, Florence. "Ada sails smoothly into 2000." Government Computer News, 07 October 1996, 33-34.

_____. "Govt. urged to perform triage in two-digit data field repairs." <u>Government Computer News</u>, 18 March 1996, 1.

Olson, Larry. "Statement," U.S. Congress. House. Science Committee. Technology Subcommittee and U.S. Congress. House. Government Reform and Oversight Committee. Government Management, Information and Technology Subcommittee. <u>Solving the Year 2000 Computer Problem</u>. Hearings. Federal Information Systems Corporation, Federal News Service, 1996.

Perlman, Ellen. "Techno-terror 2000." <u>Governing Magazine</u>, September 1996, 22.

"Preparation counts." <u>PC Week</u>, 22 July 1996, E5.

"Report: DOD's year 2000 efforts uncoordinated." <u>Phillips Business Information</u>, 04 July 1996.

Schreck, David C. "C4 Concerns for the Operational Commander." Unpublished Research Paper, U.S. Naval War College, Newport, RI: 1994.

Spiro, Leah N. "Panic in the Year Zero Zero." <u>Business Week</u>, 12 August 1996, 72-73.

Stedman, Craig. "Controversy roils over year 2000 conversion toll." <u>Computerworld</u>, 18 December 1995, 1.

Taft, Darryl K. "Toward the year 2000 -- Battling a global computer virus." <u>Computer ResellerNews</u>, 06 May 1996.

U.S. Congress. House. Science Committee. Technology Subcommittee and U.S. Congress. House. Government Reform and Oversight Committee. Government Management, Information and Technology Subcommittee. <u>Solving the Year 2000 Computer Problem</u>. Hearings. Federal Information Systems Corporation, Federal News Service, 1996.

Woodcock, Andy. "Millennium Computer melt-down 'threatens Euro'." <u>The Press Association Limited</u>, 12 September 1996.